State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

December 2, 2015

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2015-137

DATE ISSUED:
12/2/2015

SUBJECT:
Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Google Chrome, which could result in arbitrary code execution. Google Chrome is a web browser used to access the Internet. These vulnerabilities can be exploited if a user visits, or is redirected to, a specially crafted web page. Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:
- Google Chrome prior to version 47.0.2526.73
- Google V8 prior to version 4.7.80.23

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Google Chrome. These vulnerabilities can be triggered by a user visiting a specially crafted web page. Details of these vulnerabilities are as follows:

- Multiple use-after-free vulnerabilities in AppCache (CVE-2015-6765, CVE-2015-6766, CVE-2015-6767)
- Multiple cross-origin bypass vulnerabilities in DOM (CVE-2015-6768, CVE-2015-6770, CVE-2015-6772)
- A use-after-free vulnerability in DOM (CVE-2015-6777)
- A cross-origin bypass vulnerability in core (CVE-2015-6769)
- Multiple out of bounds access vulnerabilities in v8 (CVE-2015-6771, CVE-2015-6764)
- An out of bounds access vulnerability in Skia (CVE-2015-6773)
- A use-after-free vulnerability in Extensions (CVE-2015-6774)
- A type confusion vulnerability in PDFium (CVE-2015-6775)
- Multiple out of bounds access vulnerabilities in PDFium (CVE-2015-6776, CVE-2015-6778)
- A scheme bypass vulnerability in PDFium (CVE-2015-6779)
- A use-after-free vulnerability in infobars (CVE-2015-6780)
- An integer overflow vulnerability in Sfntly (CVE-2015-6781)
- A content spoofing vulnerability in Omnibox (CVE-2015-6782)
- A signature validation issue in Android Crazy Linker (CVE-2015-6783)
- An escaping issue in saved pages feature (CVE-2015-6784)
- A wildcard matching issue in CSP (CVE-2015-6785)
- A scheme bypass vulnerability in CSP (CVE-2015-6786)
- Multiple fixes from internal auditing, fuzzing and other initiatives (CVE-2015-6787)

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code in the context of the browser, obtain sensitive information, bypass security restrictions, or cause denial-of-service conditions.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches provided by Google to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:
Google:
http://googlechromereleases.blogspot.com/2015/12/stable-channel-update.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6764
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6765
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6766
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6768
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6769
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6771

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6772
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6773
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6774
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6775
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6776
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6779
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6780
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6781
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6783
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6784
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6785
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6786
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6787